

Gayle M. Blatt, SBN 122048
gmb@cglaw.com
Jeremy Robinson, SBN 188325
jrobinson@cglaw.com
P. Camille Guerra, SBN 326546
camille@cglaw.com
CASEY GERRY SCHENK
FRANCAVILLA BLATT & PENFIELD, LLP
110 Laurel Street
San Diego, CA 92101
Telephone: (619) 238-1811
Facsimile: (619) 544-9232

*Attorneys for Plaintiff
and the proposed classes*

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF CALIFORNIA**

MICHAEL MARHEFKA, on behalf
of himself and a class of others
similarly situated,

Case No.: '21 CV585 GPC AGS

**CLASS ACTION COMPLAINT
DEMAND FOR JURY TRIAL**

Plaintiff,

V.

DICKEY'S BARBECUE
RESTAURANTS, INC., a Texas
corporation,

Defendant.

1 Plaintiff Michael Marhefka, individually, and on behalf of all others
2 similarly situated, upon personal knowledge of the facts pertaining to him and on
3 information and belief as to all other matters, by and through undersigned counsel,
4 hereby brings this Class Action Complaint against Defendant Dickey's Barbecue
5 Restaurants, Inc. ("Dickey's" or "Defendant"), and alleges as follows:

6 **NATURE OF THE CASE**

7 1. Plaintiff asserts this class action against Defendant Dickey's
8 Barbecue Restaurants, Inc. for its failure to exercise reasonable care in securing
9 and safeguarding their customers' personal identifying information ("PII"),
10 including names, payment card numbers, payment card expiration dates, and
11 payment card security codes.

12 2. On October 15, 2020, a daily blog that covers computer security and
13 cybercrime, *KrebsOnSecurity.com*, revealed that payment card data had been
14 stolen from Defendant's customers at more than 100 of Defendant's restaurant
15 locations around the country (the "Data Breach").¹

16 3. The article revealed that on October 12, 2020, a "dark web" payment
17 card bazaar, "Joker's Stash," debuted a batch of more than three million stolen
18 payment card records and advertised "valid rates" of between 90 to 100 percent.
19 Companies that track the sale of stolen payment card data found one common
20 theme among all the accounts for sale: They were used at one or more of
21 Defendant's restaurants over the preceding 13 to 15 months, from May 2019
22 through September 2020.²

23 4. Gemini Advisory, a cyber intelligence firm, reported that
24 approximately 156 of Defendant's locations across 30 states likely had payment
25 systems compromised by payment card-stealing malware, with the highest

26 ¹ Krebs on Security, *Breach at Dickey's BBQ Smokes 3M Cards*, available
27 at <https://krebsonsecurity.com/2020/10/breach-at-dickeys-bbq-smokes-3m-cards/#:~:text=KrebsOnSecurity%20has%20learned%20the%20data,card%20breach%20at%20Dickey's%20BBQ>

28 ² *Id.*

1 exposure in California and Arizona. Gemini Advisory also concluded that the
2 payment transactions at Defendant's restaurants were processed via an outdated
3 magstripe method, which is prone to malware attacks.³

4 5. Defendant is no stranger to data breaches. In 2015, Defendant
5 experienced a ransomware attack that demanded \$6,000 to return the company's
6 marketing files. Following that attack, Defendant published an article detailing the
7 incident and committing to a robust cybersecurity posture. The article, complete
8 with security best practices and an endorsement of investing in proactive
9 measures, featured quotes from then-CEO Laura Rea Dickey.⁴

10 6. Despite its past experience with data security incidents and promises
11 to implement state of the art data security practices, Defendant again failed to
12 protect its customers' PII with adequate data security.

13 7. Defendant could have prevented this Data Breach. In the past few
14 years, there have been several data breaches at other restaurant chains and retail
15 establishments resulting from malware installed on point-of-sale ("POS") systems.
16 Indeed, the susceptibility of POS systems to malware is well-known throughout
17 the restaurant industry. In the last five years, practically every major data breach
18 involving retail stores or fast-food restaurant chains has been the result of malware
19 placed on POS systems. Accordingly, data security experts have warned
20 companies, "[y]our POS system is being targeted by hackers. This is a fact of
21 21st-century business."⁵ Unfortunately, Defendant's decision to ignore warnings
22 like this led to the damage alleged here.

23 8. In addition to Defendant's failure to prevent the Data Breach,
24

25 ³ Gemma Advisory, *Joker's Stash Breaches Dickey's Barbecue Pit*,
26 available at <https://geminiaidvisory.io/jokers-stash-breaches-dickeys/>

27 ⁴ Dickey.com, *DCEO: Guardians of the Network*, available at
28 <https://www.dickey.com/press/in-the-news/dceo-guardians-of-the-network>

29 ⁵ Datacap Systems Inc., *Point of sale security: Retail data breaches at a*
30 *glance*, available at <https://www.datacapsystems.com/blog/point-of-sale-security-retail-data-breaches-at-a-glance#>.

1 Defendant also failed to *detect* the breach even though it lasted for more than a
2 year.

3 9. The Data Breach was the result of Defendant's inadequate approach
4 to data security and protection of its customers' PII that it collected during the
5 course of business.

6 10. Defendant disregarded the rights of Plaintiff and the Class by
7 intentionally, willfully, recklessly, or negligently failing to take adequate and
8 reasonable measures to ensure its data systems were protected, failing to disclose
9 to its customers the material fact that it did not have adequate computer systems
10 and security practices to safeguard PII, failing to take available steps to prevent
11 the Data Breach, and failing to monitor and timely detect the Data Breach.

12 11. As a result of the Data Breach, Plaintiff's and Class members' PII has
13 been exposed to criminals for misuse. The damages to Plaintiff and the Class
14 include the following which have or may be suffered as a direct result of the Data
15 Breach:

- 16 a. unauthorized charges on debit and credit card accounts;
- 17 b. theft of personal and financial information;
- 18 c. costs associated with the detection and prevention of identity theft and
19 unauthorized use of financial accounts;
- 20 d. damages arising from the inability to use debit or credit card accounts
21 because accounts were suspended or otherwise rendered unusable as a
22 result of fraudulent charges stemming from the Data Breach,
- 23 e. damages arising from the inability to withdraw or otherwise access funds
24 because accounts were suspended, restricted, or otherwise rendered
25 unusable as a result of the Data Breach, including, but not limited to,
26 missed bill and loan payments, late-payment charges, and lowered credit
27 scores and other adverse impacts on credit;
- 28 f. costs associated with spending time to address and mitigate the actual

1 and future consequences of the Data Breach such as finding fraudulent
2 charges, cancelling and reissuing payment cards, purchasing credit
3 monitoring and identity theft protection services, imposition of
4 withdrawal and purchase limits on compromised accounts, including, but
5 not limited to, lost productivity and opportunities, time taken from the
6 enjoyment of one's life, and the inconvenience, nuisance and annoyance
7 of dealing with all issues resulting from the Data Breach;

8 g. the imminent and impending injury resulting from the potential fraud
9 and identity theft posed by PII being exposed for theft and sale on the
10 dark web

11 h. costs of products and services purchased at Defendant's various
12 restaurants during the period of the Data Breach because Plaintiff and
13 the Class would not have dined at Defendant's various restaurants had
14 Defendant disclosed that it lacked adequate systems and procedures to
15 reasonably safeguard PII; and

16 i. the loss of Plaintiff's and Class members' privacy.

17 12. The injuries Plaintiff and the Class suffered were directly and
18 proximately caused by Defendant's failure to implement or maintain adequate data
19 security measures for PII.

20 13. Plaintiff and the Class members retain a significant interest in
21 ensuring that their PII, which remains in Defendant's possession, is protected from
22 further breaches, and seek to remedy the harms suffered as a result of the Data
23 Breach for themselves and on behalf of similarly situated consumers whose PII
24 was stolen.

25 **JURISDICTION**

26 14. Subject matter jurisdiction in this civil action is authorized pursuant
27 to 28 U.S.C. § 1332(a) because the matter in controversy exceeds the sum or value
28 of \$75,000, exclusive of interest and costs, and is between citizens of different

1 states. Subject matter jurisdiction in this civil action is also authorized pursuant to
2 28 U.S.C. § 1332(d) because there are more than 100 Class members, at least one
3 class member is a citizen of a state different from that of Defendant, and the
4 amount in controversy exceeds \$5 million, exclusive of interest and costs.

5 15. The Court has personal jurisdiction over Defendant because its
6 contacts with the State of California are systematic, continuous, and sufficient to
7 subject it to personal jurisdiction in this Court. More specifically, Defendant has
8 purposefully availed itself of the privilege of conducting business in this state by
9 selling and maintaining over sixty restaurant franchises here.

10 16. Venue is proper in this district pursuant to 28 U.S.C. § 1331 because
11 a substantial part of the events and/or omissions giving rise to Plaintiff's and the
12 Class members' claims occurred within this District. Numerous class members
13 reside in this District and were therefore harmed in this District.

14 PARTIES

15 17. Plaintiff Marhefka is a citizen of the State of California and resides in
16 West Covina, California.

17 18. Defendant Dickey's Barbecue Restaurants, Inc. is a Texas
18 corporation with its principal place of business located at 4514 Cole Avenue, Suite
19 1015, Dallas, Texas 75205. Defendant operates a chain of corporate and franchise
20 restaurants known as Dickey's Barbecue Pit.

21 FACTUAL BACKGROUND

22 A. Point-of-Sale Systems

23 19. The hospitality industry – restaurants, hotels, retail stores, and
24 museums – utilize point-of-sale (“POS”) terminals or devices to process customer
25 payments for goods or services. Essentially, a POS terminal is a computerized
26 version of a cash register. POS terminals consist of a computer with specific
27 software programs that can record and track customer orders, process credit and
28 debit card transactions, connect to other systems in a network, and manage

1 inventory.

2 20. When a credit or debit card is swiped at a POS terminal, the payment
3 card data (or “PCD”) contained within a payment card is read and briefly stored in
4 the POS terminal’s memory while passing through a number of systems and
5 networks before ultimately reaching the retailer’s payment processor.

6 21. PCD is stored in a POS system’s memory in plain text and includes
7 “Track 1” and “Track 2” data from the payment card. Tracks 1 and 2 data includes
8 the cardholder’s first and last name, the card’s account number and expiration
9 date, and the card’s three-digit security code, known as the “CVV.” This
10 information, which can be used to clone credit/debit cards and to make purchases
11 online or over the telephone, is unencrypted on the payment card and thus is
12 unencrypted in the POS terminal’s memory during processing.

13 22. POS systems are particularly vulnerable to malware – which is
14 malicious software specifically designed to steal customer payment information.
15 Attacks on POS systems began in 2005. Attackers use network-sniffing malware
16 to intercept credit and debit card data during transmission to payment processors.

17 23. A malware attack is easy to implement and poses less risk to the
18 attacker in terms of detection and capture as it can be installed remotely.

19 24. All-in-one POS systems are typically based on operating systems
20 such as Windows Embedded, Windows XP and later versions, in addition to Unix
21 operating systems, such as Linux. Thus, POS systems are highly susceptible to an
22 array of attacks that can result in large data breach incidents.

23 25. For example, POS systems are vulnerable to “RAM-scraping”
24 malware, which permit attackers to exfiltrate data found in memory while the data
25 is processing inside the terminal. Software vulnerabilities are another problem
26 where there is no longer support or patches for POS systems that have older
27 running operating systems such as Windows XP or Windows XP Embedded.

28 **B. Plaintiff’s Transactions**

1 26. On or about February 3, 2020; February 25, 2020; March 18, 2020;
2 March 30, 2020; July 13, 2020; and July 27, 2020, Plaintiff Marhefka visited
3 Dickey's Barbecue Pit, one of Defendant's affected restaurants, located at 1090
4 Huntington Drive in Duarte, using his payment card.

5 27. On or about February 24, 2020 and October 13, 2020, Plaintiff
6 Marhefka visited Dickey's Barbecue Pit, one of Defendant's affected restaurants,
7 located at 2363 E. Colorado Boulevard in Pasadena, using his payment card.

8 28. Plaintiff continues to monitor his account in an effort to detect and
9 prevent misuse.

10 29. Since learning of the Data Breach, Plaintiff Marhefka has had to
11 review his account statements for fraudulent charges.

12 30. Plaintiff would not have used his payment card to make purchases at
13 Defendant's restaurants during the period of the Data Breach had Defendant
14 disclosed that they lacked adequate computer systems and data security practices
15 to safeguard customers' PII from theft.

16 31. Plaintiff suffered actual injury from having his PII stolen as a result
17 of the Data Breach.

18 32. Plaintiff suffered actual injury and damages in paying money to, and
19 purchasing products from, Defendant's restaurants during the Data Breach,
20 expenditures which he would not have made had Defendant disclosed that they
21 lacked computer systems and data security practices adequate to safeguard
22 customers' PII from theft.

23 33. Plaintiff suffered lost time, annoyance, interference, and
24 inconvenience as a result of the Data Breach, and is concerned about the loss of
25 his privacy.

26 34. Plaintiff has suffered imminent and impending injury arising from
27 the substantially increased risk of fraud, identity theft, and misuse resulting from
28 his PII being placed in the hands of criminals.

1 35. Plaintiff has a continuing interest in ensuring his PII, which remains
2 in the possession of Defendant, is protected and safeguarded from future
3 breaches.

4 **C. Dickey's Customer Data Collection Practices**

5 36. Defendant Dickey's Barbecue Restaurants, Inc. is a for-profit
6 corporation with more than 483 restaurant locations in 43 states.

7 37. As part of the dining process, Defendant's restaurants, like most
8 restaurants, accept payment cards through POS terminals, which accept customer
9 payment card data and process it for payment at the time for which a meal is paid.
10 This data includes the cardholder name, the account number, expiration date, card
11 verification value ("CVV"), and PIN data for debit cards. Defendant stores this PII
12 in the POS system and transmit this information to a third party for processing and
13 completion of the payment.

14 38. At all relevant times, Defendant was well-aware, or reasonably
15 should have been aware, that the PII collected, maintained, and stored in the POS
16 systems is highly sensitive, susceptible to attack, and could be used for wrongful
17 purposes by third parties, such as identity theft and fraud.

18 39. Such malware can go undetected for a long period of time, especially
19 if industry best practices are not routinely used.

20 40. Card payment data in particular is a valuable commodity, and there
21 is a "cyber black market" in which criminals openly post stolen payment card
22 numbers for sale.

23 41. Legitimate organizations and the criminal underground alike
24 recognize the value of PII contained in a merchant's data systems; otherwise, the
25 latter would not aggressively seek or pay for it.

26 42. Professionals tasked with trying to stop fraud and other misuse
27 know that PII has real monetary value in part because criminals continue their
28

1 efforts to obtain this data.⁶ In other words, if any additional breach of sensitive
 2 data did not have incremental value to criminals, one would expect to see a
 3 reduction in criminal efforts to obtain such additional data over time. However,
 4 just the opposite has occurred. For example, the Identity Theft Resource Center
 5 reported 1,579 data breaches in 2017, which represents a 44.7 percent increase
 6 over the record high figures reported for 2016.

7 43. The PII of consumers remains of high value to identity criminals, as
 8 evidenced by the price criminals will pay through black-market sources, or what
 9 is often called the dark web. Experian reports that a stolen credit or debit card
 10 number can sell for \$5–110 on the dark web.⁷

11 44. At all relevant times, Defendant knew, or reasonably should have
 12 known, of the importance of safeguarding PII, and of the foreseeable
 13 consequences that would occur if its data security system was breached,
 14 including, specifically, the significant costs that would be imposed on its
 15 customers as a result of a breach.

16 45. Defendant was, or should have been, fully aware of the significant
 17 volume of daily credit and debit card transactions at its restaurants, amounting to
 18 tens of thousands of daily payment card transactions, and thus, the significant
 19 number of individuals who would be harmed by a breach of Defendant's
 20 systems.

21 46. Unfortunately, and as alleged below, despite all of this publicly
 22 available knowledge of the continued compromises of PII in the hands of other
 23 third parties, such as retailers and restaurant chains, Defendant's approach to
 24 maintaining the privacy and security of Plaintiff's and Class members' PII was,

25
 26

⁶ CIO Magazine, *Data Breaches Rise as Cybercriminals Continue to Outwit IT*, available at <http://www.cio.com/article/2686167/data-breach/data-breaches-rise-as-cybercriminals-continue-to-outwit-it.html>, October 2016.

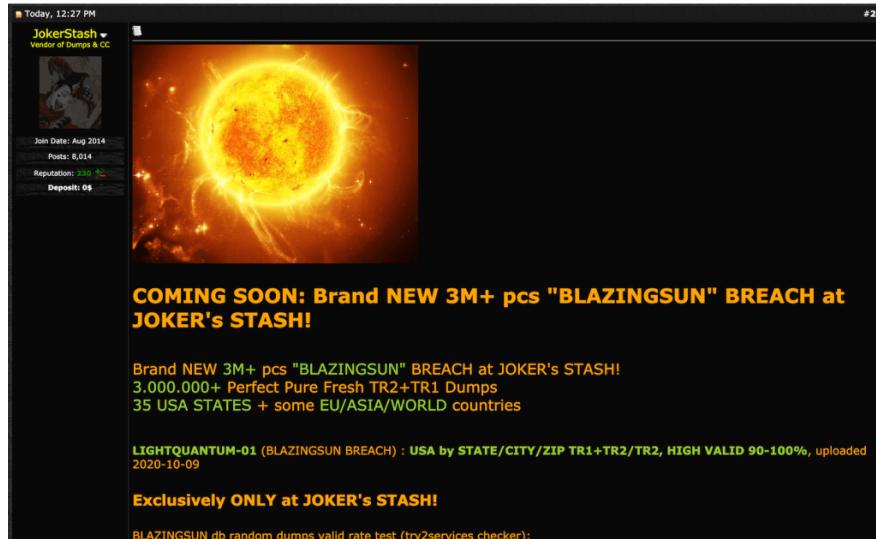
27
 28 ⁷ *Here's How Much Your Personal Information Is Selling for on the Dark Web*, available at <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/>.

1 reckless, or at the very least, negligent.

2 **D. The Data Breach**

3 47. On October 15, 2020, highly respected security blogger Brian Krebs
 4 reported that one of the dark web's most popular stores for selling stolen credit
 5 card information, "Joker's Stash," had begun selling a batch of more than 3
 6 million new card records that had been used by customers at Defendant's
 7 restaurants around the country.⁸

8 48. "Joker's Stash" originally claimed that data from the breach would be
 9 available in August and again in September. On October 12, it debuted
 10 "BlazingSun," a compilation of three million stolen card records. "Joker's Stash"
 11 advertised the card payment information as having "valid rates" of between 90 to
 12 100 percent.⁹



21 49. As explained by Krebs, the valid rates indicated that the breached
 22 merchant – Dickey's – was either unaware of the data compromise or had only
 23 just begun responding to it.¹⁰

24 50. Companies that track the sale in stolen payment card data, such as Q6
 25 Cyber and Gemini Advisory, confirmed that the card-issuing financial institutions

27 ⁸ Krebs, *supra* note 1.

28 ⁹ *Id.*

¹⁰ *Id.*

1 accounting with the accounts for sale in the BlazingSun batch had one common
2 theme: All accounts were used at various Dickey's restaurants over the preceding
3 13 to 15 months.¹¹

4 51. In its investigation of the Data Breach, Gemini Advisory concluded
5 that the widespread nature of the breach indicated that the theft may be linked to a
6 breach of Defendant's single central processor, which was used by a quarter of all
7 of Defendant's restaurant locations.¹²

8 52. Gemini Advisory further reported that it had determined that the
9 payment transactions at Defendant's restaurants were processed via the outdated
10 magstripe method, which is prone to malware attacks.¹³

11 53. Gemini Advisory reported that the financial institutions they have
12 been working with in connection with the Data Breach had already seen a
13 significant amount of fraud related to those accounts.¹⁴

14 54. Following the previously alleged 2015 ransomware incident,
15 Defendant published an article detailing the incident and committing to robust
16 cybersecurity. That article set forth data security best practices and an
17 endorsement of investing in proactive data security measures, featuring quotes
18 from its CEO at the time.¹⁵

19 55. Despite Defendant's purported commitment to data security, the
20 BlazingSun breach may contain as many as 3 million compromised card accounts
21 with a median price of \$17 per card.¹⁶ This Data Breach dwarfs the 2015
22 ransomware incident.

23 56. In addition to Defendant's failure to prevent the Data Breach,

25 ¹¹ Gemini Advisory, *supra* note 3.

26 ¹² *Id.*

27 ¹³ *Id.*

28 ¹⁴ *Id.*

¹⁵ Dickey's.com, *supra* note 4.

¹⁶ Gemini Advisory, *supra* note 3.

1 Defendant also failed to detect the breach for nearly 17 months. Intruders,
2 therefore, had months to collect PII unabated. During this time, Defendant failed
3 to recognize that its systems had been breached and that intruders were stealing
4 data on millions of payment cards. Timely action by Defendant likely would
5 have significantly reduced the consequences of the breach. Instead, Defendant
6 took more than 17 months to realize that its systems had been breached, and thus
7 contributed to the scale of the Data Breach and the resulting damages to Plaintiff
8 and Class members.

9 57. While many merchants and vendors have responded to recent data
10 breaches by adopting technology and security practices that help make
11 transactions and stored data more secure, Defendant failed to do so. Instead,
12 Defendant's restaurants continued to use the outdated magstripe method to
13 process customers' purchases. This outdated magstripe method is prone to
14 malware attacks.¹⁷

15 58. Additionally, based on information and belief, Defendant did not
16 provide written notice to consumers affected by the POS malware attack.

17 **E. Defendant Failed to Comply with Industry Standards**

18 59. Despite the enumerated vulnerabilities of POS systems, available
19 security measures, and reasonable business practices would have significantly
20 reduced or even eliminated the likelihood that hackers could successfully infiltrate
21 a business' POS system. The payment card networks (MasterCard, Visa, Discover,
22 and American Express), data security organizations, state governments, and
23 federal agencies have all implemented various standards and guidance on security
24 measures designed to prevent these types of intrusions into POS systems.
25 However, despite Defendant's understanding of the risk of data theft via malware
26 installed on POS systems, and the widely available resources to prevent intrusion
27 into POS data systems, Defendant failed to adhere to these guidelines and failed to

28 ¹⁷ *Id.*

1 take reasonable and sufficient protective measures to prevent the Data Breach.

2 60. Security experts have recommended specific steps that retailers
3 should take to protect their POS systems. For example, a few years ago, Symantec
4 recommended “point to point encryption” implemented through secure card
5 readers, which encrypt credit card information in the POS system, preventing
6 malware that extracts card information through the POS memory while it
7 processes the transaction.¹⁸ Moreover, Symantec emphasized the importance of
8 adopting EMV (Europay, Visa, and Mastercard) chip technology. Datacap
9 Systems, a developer of POS systems, recommended similar preventative
10 measures.¹⁹

11 61. Credit card companies announced that retailers must use EMV chip
12 reading machines by October 1, 2015 instead of swiping machines. EMV
13 payment cards contain a microchip that is used to improve payment security and
14 prevent counterfeit card fraud. Consumers insert their cards into the front of a
15 card reader with the metallic square chip facing up instead of swiping cards.
16 Cards with magnetic strips contain unchanging data that can easily be replicated
17 over and over again, unlike the chip cards that create a unique transaction code
18 that cannot be used again. If an attacker steals the chip data from a specific point
19 of sale, card duplication is unavailable because the stolen transaction number
20 created would not be usable again.

21 62. Upon information and belief, Defendant failed to use EMV chips at
22 many of its restaurants to process customers’ transactions, and instead used an
23 outdated magstripe method. The outdated magstripe method used by Defendant
24 is prone to malware attacks.²⁰

25
26 ¹⁸ Symantec, *A Special Report On Attacks On Point-of-Sale Systems*, p. 3
27 (Nov. 20, 2014), available at <https://docs.broadcom.com/doc/attacks-on-point-of-sale-systems-en>

28 ¹⁹ DataCap Systems, *supra* note 5.

20 Gemini Advisory, *supra* note 3

1 63. The major payment card industry brands set forth specific security
 2 measures in their Card (or sometimes, Merchant) Operating Regulations. Card
 3 Operating Regulations are binding on merchants and require merchants to: (1)
 4 protect cardholder data and prevent its unauthorized disclosure; (2) store data,
 5 even in encrypted form, no longer than necessary to process the transaction; and
 6 (3) comply with all industry standards.

7 64. The Payment Card Industry Data Security Standard (“PCI DSS”) is
 8 a set of requirements designed to ensure that companies maintain consumer
 9 credit and debit card information in a secure environment.²¹

10 65. The PCI DSS “was developed to encourage and enhance cardholder
 11 data security” by providing “a baseline of technical and operational requirements
 12 designed to protect account data.”²² PCI DSS sets the minimum level of what
 13 must be done, not the maximum.

14 65. PCI DSS 3.2 imposes the following requirements on Defendant:²³

PCI Data Security Standard – High Level Overview	
Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

21 Payment Card Industry Data Security Standard v3.2, at 5 (April 2016) available at https://www.pcihispano.com/contenido/uploads/2016/09/PCI_DSS_v3-2-1.pdf

22 *Id.*

23 *Id.*

1 66. Among other things, PCI DSS required Defendant to properly secure
2 and protect payment card data; not store cardholder data beyond the time
3 necessary to authorize a transaction; maintain up-to-date antivirus software and a
4 proper firewall; protect systems against malware; establish a process to identify
5 and timely fix security vulnerabilities; and encrypt payment card data at the point
6 of sale.

7 67. PCI DSS also required Defendant not to store “the full contents
8 of...the magnetic stripe located on the back of a card” or “the card verification
9 code or value” after authorization.²⁴ Despite understanding the consequences of
10 inadequate data security, Defendant failed to comply with PCI DSS requirements
11 and failed to take additional protective measures beyond those required by PCI
12 DSS.

13 **F. Defendant Failed to Comply with Federal and State Requirements**

14 68. Federal and State governments have likewise established security
15 standards and issued recommendations to temper data breaches and the resulting
16 harm to consumers and financial institutions.

17 69. There are a number of state and federal laws and requirements and
18 industry standards governing the protection of payment card data.

19 70. For example, at least 24 states have enacted laws addressing data
20 security practices that require that businesses that own, license or maintain
21 personal information about a resident of that state to implement and maintain
22 “reasonable security procedures and practices” and to protect personal information
23 from unauthorized access. California is one such state and, per the California
24 Consumer Privacy Act, requires that “A business that owns, license, or maintains
25 personal information about a California resident shall implement and maintain
26 reasonable security procedures appropriate to the nature of the information, to
27 protect the personal information from unauthorized access, destruction, use

28 ²⁴ *Id.* at 38 (PCI DSS 3.2.1 and 3.2.2).

1 modification or disclosure.” Cal. Civ. Code § 1798.81.5(b). Personal information
 2 under these statutes usually is defined to include an individual’s first name or
 3 initial and last name in combination with a credit or debit card number that is in
 4 combination with any required security code, access code, or password that would
 5 permit access to the individual’s financial account. See, e.g., Cal. Civ. Code §
 6 1798.81.5(d)(1)(A)(iii).

7 71. The Federal Trade Commission (“FTC”) has issued numerous
 8 guides for business highlighting the importance of reasonable data security
 9 practices. According to the FTC, the need for data security should be factored
 10 into all business decision-making.²⁵

11 72. In 2016, the FTC updated its publication, *Protecting Personal*
 12 *Information: A Guide for Business*, which established guidelines for fundamental
 13 data security principles and practices for business.²⁶ The guidelines note
 14 businesses should protect the personal customer information that they keep;
 15 properly dispose of personal information that is no longer needed; encrypt
 16 information stored on computer networks; understand their network’s
 17 vulnerabilities; and implement policies to correct security problems. The
 18 guidelines also recommend that businesses use an intrusion detection system to
 19 expose a breach as soon as it occurs; monitor all incoming traffic for activity
 20 indicating someone is attempting to hack the system; watch for large amounts of
 21 data being transmitted from the system; and have a response plan ready in the
 22 event of a breach.

23 73. The FTC recommends that companies not maintain cardholder
 24 information longer than is needed for authorization of a transaction; limit access
 25

26²⁵ Federal Trade Commission, *Start With Security*, available at
<https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf>

27²⁶ Federal Trade Commission, *Protecting Personal Information: A Guide*
 28 *for Business*, available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf

1 to sensitive data; require complex passwords to be used on networks; use
2 industry-tested methods for security; monitor for suspicious activity on the
3 network; and verify that third-party service providers have implemented
4 reasonable security measures.²⁷

5 74. The FTC has brought enforcement actions against businesses for
6 failing to adequately and reasonably protect customer data, treating the failure to
7 employ reasonable and appropriate measures to protect against unauthorized
8 access to confidential consumer data as an unfair act or practice prohibited by
9 Section 5 of the Federal Trade Commission Act (“FTCA”), 15 U.S.C. § 45.
10 Orders resulting from these actions further clarify the measures businesses must
11 take to meet their data security obligations.

12 75. Defendant’s failure to employ reasonable and appropriate measures
13 to protect against unauthorized access to confidential consumer data constitutes
14 an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

15 76. In this case, Defendant was at all times fully aware of its obligation
16 to protect the PII of customers because of its participation in payment card
17 processing networks. Defendant was also aware of the significant repercussions
18 if it failed to do so because Defendant collected payment card data from tens of
19 thousands of customers daily and they knew that this data, if hacked, would
20 result in injury to consumers, including Plaintiff and Class members.

21 77. Despite understanding the consequences of inadequate data security,
22 Defendant operated POS systems with the outdated magstripe method; failed to
23 enable point-to-point and end-to-end encryption and failed to take other
24 measures necessary to protect its data network.

25 **G. Plaintiff and Class Members Are Damaged**

26 78. The PII of Plaintiff and Class members is private and sensitive in
27 nature and was left inadequately protected by Defendant. Defendant did not obtain

28 ²⁷ Federal Trade Commission, *supra* note 26.

1 Plaintiff's and Class members' consent to disclose PII to any other person as
2 required by applicable law and industry standards.

3 79. Defendant also failed to notify Plaintiff and Class Members of the
4 Data Breach, in direct violation of data breach notification laws, such as California
5 Civil Code § 1798.82.

6 80. The Data Breach was a direct and proximate result of Defendant's
7 failure to properly safeguard and protect Plaintiff's and Class members' PII from
8 unauthorized access, use, and disclosure, as required by various state and federal
9 regulations, industry practices, and the common law, including Defendant's failure
10 to establish and implement appropriate administrative, technical, and physical
11 safeguards to ensure the security and confidentiality of Plaintiff's and Class
12 members' PII to protect against reasonably foreseeable threats to the security or
13 integrity of such information.

14 81. Had Defendant remedied the deficiencies in its POS systems,
15 followed PCI DSS guidelines, and adopted security measures recommended by
16 experts in the field, Defendant would have prevented intrusion into its POS
17 systems and, ultimately, the theft of customers' PII.

18 82. As a result of Defendant's wrongful actions, inaction, negligent
19 security practices, and the resulting Data Breach, Plaintiff and Class members
20 have been placed at an imminent, immediate, and continuing increased risk of
21 harm from identity theft and identity fraud, requiring them to take the time which
22 they otherwise would have dedicated to other life demands such as work and
23 family in an effort to mitigate the actual and potential impact of the Data Breach
24 on their lives including, *inter alia*, by placing "freezes" and "alerts" with credit
25 reporting agencies, contacting their financial institutions, closing or modifying
26 financial accounts, closely reviewing and monitoring their credit reports and
27 accounts for unauthorized activity, and filing police reports. This time has been
28 lost forever and cannot be recaptured.

1 83. Defendant's wrongful actions and inaction directly and proximately
2 caused the theft and dissemination into the public domain of Plaintiff's and Class
3 members' PII, causing them to suffer, and continue to suffer, economic damages
4 and other actual harm for which they are entitled to compensation, including:

- 5 a. unauthorized charges on debit and credit card accounts;
- 6 b. theft of personal and financial information;
- 7 c. costs associated with the detection and prevention of identity theft and
8 unauthorized use of financial accounts;
- 9 d. damages arising from the inability to use debit or credit card accounts
10 because accounts were suspended or otherwise rendered unusable as a
11 result of fraudulent charges stemming from the Data Breach;
- 12 e. damages arising from the inability to withdraw or otherwise access funds
13 because accounts were suspended, restricted, or otherwise rendered
14 unusable as a result of the Data Breach, including, but not limited to,
15 missed bill and loan payments, late-payment charges, and lowered credit
16 scores and other adverse impacts on credit;
- 17 f. costs associated with spending time to address and mitigate the actual
18 and future consequences of the Data Breach such as finding fraudulent
19 charges, cancelling and reissuing payment cards, purchasing credit
20 monitoring and identity theft protection services, imposition of
21 withdrawal and purchase limits on compromised accounts, including, but
22 not limited to, lost productivity and opportunity(ies), time taken from the
23 enjoyment of one's life, and the inconvenience, nuisance and annoyance
24 of dealing with all issues resulting from the Data Breach;
- 25 g. imminent and impending injury resulting from the potential fraud and
26 identity theft posed by PII being exposed for theft and sale on the dark
27 web;

28

- h. loss of use of, and access to, their account funds and costs associated with the inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including adverse credit notations; and
- i. the loss of Plaintiff's and Class members' privacy.

7 84. While Plaintiff's and Class members' PII has been stolen, Defendant
8 continues to hold PII of consumers, including Plaintiff and Class members.
9 Because Defendant has demonstrated an inability to prevent a breach or stop it
10 from continuing even after being detected, Plaintiff and Class members have a
11 strong interest in ensuring that their PII is secure, remains secure, is properly and
12 promptly destroyed, and is not subject to further theft.

CLASS ACTION ALLEGATIONS

14 85. Plaintiff brings this lawsuit as a class action on behalf of himself and
15 all others similarly situated as members of the proposed classes pursuant to
16 Federal Rules of Civil Procedure 23(a) and 23(b)(3):

A. The Nationwide Class

18 86. Plaintiff seeks to represent a class comprised of United States
19 residents (the “Nationwide Class”), defined as follows:

20 All persons residing in the United States who made a credit or debit
21 card purchase at any affected Dickey's Barbecue Pit restaurant during
22 the period of the Data Breach.

B. The California Subclass

24 87. Plaintiff seeks to represent a class comprised of California residents
25 (the “California Subclass”), defined as follows:

26 All persons residing in the State of California who made a credit or
27 debit card purchase at any affected Dickey's Barbecue Pit restaurant
28 during the period of the Data Breach.

1 88. Collectively, the Nationwide Class and California Subclass will be
2 referred to as “the Class” except where there is need to distinguish the class and
3 subclass.

4 89. Excluded from the proposed Class are Defendant, including any
5 entity in which Defendant has a controlling interest, is a subsidiary, or which is
6 controlled by Defendant, as well as the officers, directors, affiliates, legal
7 representatives, heirs, predecessors, successors, and assigns of Defendant.

8 90. Plaintiff reserves the right to amend or modify the class definitions
9 with greater specificity or division after having had an opportunity to conduct
10 discovery.

11 91. **Numerosity:** Although the exact number of Class members is
12 uncertain and can only be ascertained through appropriate discovery, the number
13 is great enough – with the Data Breach impacting approximately 3 million
14 customer accounts - such that joinder is impracticable. The disposition of the
15 claims of these Class members in a single action will provide substantial benefits
16 to all parties and to the Court. The Class members may be identifiable from
17 objective means, such as information and records in Defendant’s possession,
18 custody, or control.

19 92. **Commonality and Predominance.** Common questions of law and
20 fact exist as to the proposed Class members and predominate over questions
21 affecting only individual Class members. These common questions include:

- 22 a. Whether Defendant engaged in the wrongful conduct alleged herein;
- 23 b. Whether Defendant’s security measures to protect their POS systems
24 were reasonable in light of the PCI DSS requirements, FTC data security
25 recommendations, and best practices recommended by data security
26 experts;
- 27 c. Whether Defendant’s failure to implement adequate data security
28 measures resulted in or was the proximate cause of the breach of its POS

1 data systems;

2 d. Whether Defendant's conduct, including their failure to act, resulted in
3 or was the proximate cause of the breach of the POS systems, resulting
4 in the loss of PII of Plaintiff and Class members;

5 e. Whether Defendant owed a legal duty to Plaintiff and the other Class
6 members to exercise due care in collecting, storing, and safeguarding
7 their PII;

8 f. Whether Defendant negligently or recklessly breached legal duties owed
9 to Plaintiff and the other Class members to exercise due care in
10 collecting, storing, and safeguarding their PII;

11 g. Whether Plaintiff and the Class are at an increased risk for identity theft
12 because of the Data Breach;

13 h. Whether Defendant's conduct violated Cal. Bus. & Prof. Code § 17200,
14 et seq.;

15 i. Whether Defendant violated section 1798.150 of the California
16 Consumer Privacy Act by failing to prevent Plaintiff's and Class
17 members' nonencrypted and nonredacted PII from unauthorized access
18 and exfiltration, theft, or disclosure, as a result of Defendant's violations
19 of their duty to implement and maintain reasonable security procedures
20 and practices appropriate to the nature of the information;

21 j. Whether Plaintiff and the other Class members are entitled to actual,
22 statutory, or other forms of damages, and other monetary relief; and

23 k. Whether Plaintiff and the other Class members are entitled to equitable
24 relief, including, but not limited to, injunctive relief and restitution.

25 93. Defendant engaged in a common course of conduct giving rise to the
26 legal rights sought to be enforced by Plaintiff individually and on behalf of the
27 other Class members. Individual questions, if any, pale by comparison, in both
28 quantity and quality, to the numerous questions that dominate this action.

1 94. **Typicality:** Plaintiff's claims are typical of the claims of the
2 members of the Classes. Plaintiff is a consumer who used his payment card at an
3 affected Dickey's restaurant locations and had his payment card data
4 compromised as a result of the Data Breach. Plaintiff's damages and injuries are
5 akin to other Class members, and Plaintiff seeks relief consistent with the relief of
6 the Class members.

7 95. **Adequacy of Representation:** Plaintiff is an adequate representative
8 of the Class because his interests do not conflict with the interests of the other
9 Class members he seeks to represent; he has retained counsel competent and
10 experienced in complex class action litigation, and Plaintiff will prosecute this
11 action vigorously. The interests of the Class will be fairly and adequately
12 protected by Plaintiff and Plaintiff's counsel.

13 96. **Superiority:** A class action is superior to any other available means
14 for the fair and efficient adjudication of this controversy, and no unusual
15 difficulties are likely to be encountered in the management of this matter as a class
16 action. The damages, harm, or other financial detriment suffered individually by
17 Plaintiff and the other Class members are relatively small compared to the burden
18 and expense that would be required to litigate their claims on an individual basis
19 against Defendant, making it impracticable for Class members to individually seek
20 redress for Defendant's wrongful conduct. Even if Class members could afford
21 individual litigation, the court system could not. Individualized litigation would
22 create a potential for inconsistent or contradictory judgments and increase the
23 delay and expense to all parties and the court system. By contrast, the class action
24 device presents far fewer management difficulties and provides the benefits of
25 single adjudication, economies of scale, and comprehensive supervision by a
26 single court.

27
28

1 **COUNT I**

2 Negligence

3 **(On Behalf of Plaintiff and the Nationwide Class)**

4 97. Plaintiff incorporates by reference all allegations in this Complaint as
though fully set forth herein.

5 98. Defendant solicited and took possession of Plaintiff's and the Class
6 members' PII, and Defendant had a duty to exercise reasonable care in securing
7 that information from unauthorized access or disclosure. Defendant also had a
8 duty to timely notify Plaintiff and the Class that their PII had been or may have
9 been stolen. Defendant further had a duty to destroy Plaintiff's and Class
10 members' PII within an appropriate amount of time after it was no longer required
11 by Defendant, in order to mitigate the risk of such non-essential PII being
12 compromised in a data breach.

13 99. Upon accepting and storing Plaintiff's and Class members' PII in its
14 computer systems and on its networks, Defendant undertook and owed a duty of
15 care to Plaintiff and Class members to exercise reasonable care to secure and
16 safeguard Plaintiff's and Class members' PII and to use commercially-reasonable
17 methods to do so. Defendant knew that the PII was private and confidential and
18 should be protected as private and confidential.

19 100. Defendant owed a duty of care to not subject Plaintiff and Class
20 members, along with their PII, to an unreasonable risk of harm because they were
21 foreseeable and probable victims of inadequate security practices.

22 101. Defendant owed a duty of care to Plaintiff and Class members to
23 quickly detect a data breach and to timely act on warnings about data breaches.

24 102. Defendant's duties arose from its relationship to Plaintiff and Class
25 members and from industry custom.

26 103. Defendant, through its actions and/or failures to act, unlawfully
27 breached duties to Plaintiff and Class members by failing to implement standard

1 industry protocols and to exercise reasonable care to secure and keep private the
2 PII entrusted to it.

3 104. Defendant, through its actions and/or failures to act, allowed
4 unmonitored and unrestricted access to its customers' unsecured PII.

5 105. Defendant, through its actions and/or failures to act, failed to provide
6 adequate supervision and oversight of the PII with which it was entrusted, despite
7 knowing the risk and foreseeable likelihood of a breach and misuse, which
8 permitted unknown third parties to gather Plaintiff's and Class members' PII,
9 misuse that PII, and intentionally disclose it to unauthorized third parties without
10 consent.

11 106. Defendant knew, or should have known, the risks inherent in
12 collecting and storing PII, the vulnerabilities of POS systems, and the importance
13 of adequate security. Defendant was aware, or should have been aware, of
14 numerous, well-publicized data breaches within the restaurant industry.

15 107. Defendant knew, or should have known, that its data systems and
16 networks did not adequately safeguard Plaintiff's and Class members' PII.

17 108. Due to Defendant's knowledge that a breach of its systems could
18 damage millions of its customers, including Plaintiff and Class members,
19 Defendant had a duty to adequately protect its data systems and the PII contained
20 therein.

21 109. Defendant's own conduct also created a foreseeable risk of harm to
22 Plaintiff and Class members and their PII. Defendant's misconduct included
23 failing to: (1) secure the POS systems, despite knowing its vulnerabilities; (2)
24 comply with industry standard security practices; (3) implement adequate system
25 and event monitoring; and (4) implement the systems, policies, and procedures
26 necessary to prevent this type of data breach.

27
28

1 110. Defendant also had independent duties under state and federal laws
2 that required Defendant to reasonably safeguard Plaintiff's and Class members'
3 PII, and promptly notify them about the Data Breach.

4 111. Defendant breached its duties to Plaintiff and Class members in
5 numerous ways, including:

- 6 a. by failing to provide fair, reasonable, or adequate computer systems and
7 data security practices to safeguard Plaintiff's and Class members' PII;
- 8 b. by creating a foreseeable risk of harm through the misconduct previously
9 described;
- 10 c. by failing to comply with industry standard data security standards
11 during the period of the Data Breach; and
- 12 d. by failing to timely and accurately disclose that Plaintiff's and Class
13 members' PII had been improperly acquired or accessed.

14 112. Through Defendant's acts and omissions described in this Complaint,
15 including Defendant's failure to provide adequate security and its failure to protect
16 Plaintiff's and Class members' PII from being foreseeably captured, accessed,
17 disseminated, stolen, and misused, Defendant unlawfully breached its duties to use
18 reasonable care to adequately protect and secure Plaintiff's and Class members'
19 PII while it was within Defendant's possession or control.

20 113. Upon information and belief, Defendant improperly and inadequately
21 safeguarded Plaintiff's and Class members' PII in deviation of standard industry
22 rules, regulations, and practices at the time of the unauthorized access.
23 Defendant's failure to take proper security measures to protect customers' PII as
24 described in this Complaint, created conditions conducive to a foreseeable,
25 intentional criminal act, namely the unauthorized access of Plaintiff's and Class
26 members' PII.

27 114. In engaging in the negligent acts and omissions as alleged herein,
28 which permitted an unknown third party to access Defendant's customers' PII,

1 Defendant violated Section 5 of the FTC Act, which prohibits “unfair...practices
2 in or affecting commerce.” This prohibition includes failing to have adequate data
3 security measures and failing to protect their customers’ PII.

4 115. Plaintiff and the Class members are among the class of persons
5 Section 5 of the FTC Act was designed to protect, and the injuries suffered by
6 Plaintiff and the Class members is the type of injury Section 5 of the FTC Act was
7 intended to prevent. As a result, Defendant is negligent per se.

8 116. Neither Plaintiff nor the other Class members contributed to the Data
9 Breach and subsequent misuse of their PII as described in this Complaint.

10 117. Defendant’s failure to exercise reasonable care in safeguarding PII by
11 adopting appropriate security measures was the direct and proximate cause of
12 Plaintiff’s and Class members’ PII being accessed and stolen through the data
13 breach.

14 118. Defendant breached its duties to Plaintiff and Class members by
15 failing to provide fair, reasonable, and adequate computer systems and data
16 security practices to safeguard Plaintiff’s and Class members’ PII.

17 119. As a result of Defendant’s breach of its duties, Plaintiff and the Class
18 members suffered or are at increased risk of suffering damages including, but not
19 limited to: loss of right to privacy of PII, damages arising from the unauthorized
20 charges on their debit or credit cards or on cards that were fraudulently obtained
21 through the use of their PII; damages arising from Plaintiff’s and Class members’
22 inability to use their debit or credit cards because those cards were cancelled,
23 suspended, or otherwise rendered unusable as a result of the Data Breach and/or
24 false or fraudulent charges stemming from the Data Breach, including but not
25 limited to late fees charged and foregone cash back rewards; damages from lost
26 time and effort to mitigate the actual and potential impact of the Data Breach on
27 their lives including, inter alia, by placing “freezes” and “alerts” with credit
28 reporting agencies, contacting their financial institutions, closing or modifying

1 financial accounts, closely reviewing and monitoring their credit reports and
2 accounts for unauthorized activity, and filing police reports, and damages from
3 identity theft, which may take months if not years to discover and detect, given the
4 far-reaching, adverse and detrimental consequences of identity theft and loss of
5 privacy. The nature of other forms of economic damage and injury may take years
6 to detect, and the potential scope can only be assessed after a thorough
7 investigation of the facts and events surrounding the theft mentioned above.

8 **COUNT II**

9 **Violations of California's Unfair Competition Law**

10 **Cal. Bus. & Prof. Code § 17200, *et seq.***

11 **(On Behalf of Plaintiff and the Nationwide Class)**

120. Plaintiff incorporates by reference all allegations in this Complaint as
11 though fully set forth herein.

121. Defendant's business practices as complained of herein violate the
13 Unfair Competition Law, Cal. Bus. & Prof. Code § 17200, *et seq.* ("UCL").

122. Defendant's practices constitute "unlawful" business practices in
15 violation of the UCL because, among other things, they violate statutory law and
16 the common law, including without limitation the California Consumer Privacy
17 Act, Cal. Civ. Code § 1798.150 and Section 5 of the FTC Act.

123. Defendant's actions and practices constitute "unfair" business
19 practices in violation of the UCL, because, among other things, the gravity of the
20 harm to Plaintiff and the Class members outweighs the utility of Defendant's
21 conduct. This conduct includes Defendant's failure to adequately ensure the
22 privacy, confidentiality, and security of customers' data entrusted to it and
23 Defendant's failure to have adequate data security measures in place.

124. As a result of Defendant's wrongful business practices, Plaintiff and
25 members of the Class have suffered injury in fact and lost money or property as
26 alleged herein.

125. Defendant's wrongful business practices present an ongoing and continuing threat to the general public.

126. Accordingly, Plaintiff and Class members have and will incur economic damages related to the breach including, time and money spent remediating the breach, monitoring their financial accounts to ensure no further fraud or no fraud is perpetuated; time spent insuring that any unauthorized charges are identified and remedied; experiencing lack of access to funds while banks and financial institutions issue new cards; and the costs of credit monitoring, purchasing credit reports, and purchasing “freezes” to prevent opening of unauthorized accounts.

COUNT III
Violation of the California Consumer Privacy Act
Cal. Civ. Code § 1798.150
(On Behalf of Plaintiff and the California Subclass)

127. Plaintiff incorporates by reference all allegations in this Complaint as though fully set forth herein.

128. Defendant collects consumers' personal information as defined in Cal. Civ. Code § 1798.140. As a result, Defendant has a duty to implement and maintain reasonable security procedures and practices to protect this personal information. As alleged herein, Defendant failed to do so.

129. Defendant violated § 1798.150 of the California Consumer Privacy Act (“CCPA”) by failing to prevent Plaintiff and Class members’ nonencrypted and nonredacted PII from unauthorized access and exfiltration, theft, or disclosure. These failures were the result of Defendant’s violations of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information.

130. As a direct and proximate result of Defendant's conduct, Plaintiff and the Class members' PII, including names, payment card numbers, payment card expiration dates, and payment card security codes, was subjected to unauthorized

access, exfiltration, and theft. On information and belief, Plaintiff and the Class allege this PII was not encrypted or redacted in the format accessed during the Data Breach.

131. Plaintiff and the Class members seek injunctive or other equitable relief to ensure Defendant hereafter adequately safeguards customers' PII by implementing reasonable security procedures and practices. Such relief is particularly important because Defendant continues to hold customers' PII, including that of Plaintiff and the California Subclass. These individuals have an interest in ensuring that their PII is reasonably protected.

132. On April 5, 2021, Plaintiff’s Counsel sent a notice letter to Defendant Dickey’s Barbecue Restaurants, Inc.’s registered service agent via FedEx Priority. Assuming Defendant cannot cure the Data Breach within 30 days, and Plaintiff believes any such cure is not possible under these facts and circumstances, Plaintiff intends to promptly amend this complaint to seek actual damages and statutory damages of no less than \$100 and up to \$750 per customer record subject to the Data Breach on behalf of the California Subclass as authorized by the CCPA.

COUNT IV
Declaratory Judgment
(On Behalf of Plaintiff and the California Subclass)

133. Plaintiff incorporates by reference all allegations in this Complaint as though fully set forth herein.

134. There exists a controversy regarding the reasonableness of the security measures Defendant provided as applicable to Plaintiff's claim under the CCPA.

135. A judicial determination addressing the issues is necessary now to avoid additional data breaches due to insufficient security protection.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all others similarly

1 situated, respectfully requests that the Court enter an order:

2 a. Certifying the proposed Class as requested herein;

3 b. Appointing Plaintiff as Class Representative and undersigned counsel as

4 Class Counsel;

5 c. Finding that Defendant engaged in the unlawful conduct as alleged herein;

6 d. Enjoining Defendant's conduct and requiring Defendant to implement

7 proper data security policies and practices;

8 e. Awarding Plaintiff and Class members damages;

9 f. Awarding Plaintiff and Class members pre-judgment and post-judgment

10 interest on all amounts awarded;

11 g. Awarding Plaintiff and the Class members reasonable attorneys' fees, costs,

12 and expenses; and

13 h. Granting such other relief as the Court deems just and proper.

14

15 **DEMAND FOR JURY TRIAL**

16 Plaintiff, on behalf of himself and the proposed Class, hereby demands a

17 trial by jury as to all matters so triable.

18

19 Dated: April 5, 2021

/s/ Gayle M. Blatt
GAYLE M. BLATT

21 **CASEY GERRY SCHENK**
22 **FRANCAVILLA BLATT &**
23 **PENFIELD, LLP**

24 *Attorneys for Plaintiff and the*
putative Classes

25
26
27
28